In the Claims

1. (Cancelled)

2. (Currently amended) The computerized method of claim ~~1~~ 1, wherein the data structure is a directory entry for the file and the anti-virus state information is stored in at least one field in the directory entry.

3. (Currently amended) ~~The~~ A computerized method for fast virus scanning of a file ~~of claim 2, further~~ comprising:

storing anti-virus state information in a data structure associated with the file and managed by a file system;

partitioning the anti-virus state information into segments when storing the anti-virus state information in non-contiguous fields in the data structure, each segment being equal in size to one of a plurality of fields in the ~~directory entry~~data structure; and

obtaining the anti-virus state information for the file from the data structure when the data structure has been retrieved by the file system.

4. (Currently amended) The computerized method of claim 2, further comprising:

creating the at least one field in the directory entry.

5. (Currently amended) The computerized method of claim ~~1~~ 1, wherein the data structure is an extra file fork for the file.

6. (Original) The computerized method of claim ~~5~~ 4, further comprising creating the extra file fork to hold the anti-virus state information.

7. (Currently amended) The computerized method of claim ~~1~~ 1, wherein the data structure is stored as a resource within a resource fork for the file.

7.
~~8.~~ (Currently amended) The computerized method of claim ~~12~~ 1, further comprising:

encrypting the anti-virus state information before storing it in the data structure; and

decrypting the anti-virus state information when it is obtained from the data structure.

8.
~~9.~~ (Currently amended) The computerized method of claim ~~12~~ 1, further comprising:

comparing the anti-virus state information stored in the data structure against corresponding information associated with a current version of the file to determine if virus scanning is required; and

updating the anti-virus state information if the file is scanned as a result of the comparison.

9.
~~10.~~ (Currently amended) The computerized method of claim ~~13~~ 1, wherein data structure is retrieved by the file system as a result of the file being accessed by an application program.

a1

10.
~~11.~~ (Currently amended) The computerized method of claim ~~13~~ 1, wherein data structure is retrieved by the file system as a result of a user requesting the file be scanned.

11.
~~12.~~ (Currently amended) The computerized method of claim ~~13~~ 1, wherein data structure is retrieved by the file system as a result of the file being in a pre-defined list of files scheduled for scanning.

12.
~~13.~~ (Currently amended) A computer-readable medium having stored thereon executable instructions that cause a computer to execute a virus scanning method on a file, the method comprising:

storing anti-virus state information for the file in a data structure associated with the file and managed by a file system;

A

partitioning the anti-virus state information into segments when storing the anti-virus state information in non-contiguous fields in the data structure, each segment being equal in size to one of a plurality of fields in the data structure; and

obtaining the anti-virus state information for the file from the data structure when the data structure has been retrieved by the file system.

13. ~~14.~~ (Original) The computer-readable medium of claim ~~13~~ 12, further comprising:

encrypting the anti-virus state information before storing it in the data structure; and

decrypting the anti-virus state information when it is obtained from the data structure.

14. ~~15.~~ (Original) The computer-readable medium of claim ~~13~~ 12, further comprising:

comparing the anti-virus state information stored in the data structure against corresponding information associated with a current version of the file to determine if virus scanning is required; and

updating the anti-virus state information if the file is scanned as a result of the comparison.

15. ~~16.~~ (Currently amended) The computer-readable medium of claim ~~13~~ 12, wherein the data structure is a directory entry for the file and the anti-virus state information is stored in at least one field in the directory entry.

16. ~~17.~~ (Original) The computer-readable medium of claim ~~13~~ 12, wherein the data structure is an extra file fork for the file.

17. ~~18.~~ (Original) The computer-readable medium of claim ~~17~~ 16, further comprising:

creating the extra file fork to hold the anti-virus state information.

18. ~~19.~~ (Currently amended) A computer system comprising:

a processor coupled to a system bus;

a memory coupled to the processor through the system bus;

a computer-readable medium coupled to the processor through the system bus;

a file system executed from the ~~computer readable medium~~ memory by the processor, wherein the file system causes the processor to store data structures associated with files on the computer-readable medium and further to retrieve the data structures from the computer-readable medium; and

an anti-virus process executed from the ~~computer readable medium~~ memory by the processor, wherein the anti-virus process causes the processor to store anti-virus state information for the file in the data structure associated with the file, partition the anti-virus state information into segments when storing the anti-virus state information in non-contiguous fields in the data structure, each segment being equal in size to one of a plurality of fields in the data structure; and further to obtain the anti-virus state information for the file from the data structure when the data structure has been retrieved.

19. 18
~~20~~. (Currently amended) The computer system of claim ~~20~~19, wherein the anti-virus process further causes the processor to encrypt the anti-virus state information before storing it in the data structure and to decrypt the anti-virus state information when it is obtained from the data structure.

20. 18
~~21~~. (Currently amended) The computer system of claim ~~20~~19, wherein the anti-virus process further causes the processor to compare the anti-virus state information stored in the data structure against corresponding information associated with a current version of the file to determine if virus scanning is required and to update the anti-virus state information if the anti-virus process causes the processor to scan the file as a result of the comparison.

21. 18
~~22~~. (Currently amended) The computer system of claim ~~20~~19, wherein the data structure containing the anti-virus state information is an entry in a file system directory and the anti-virus process further causes the processor to store the anti-virus state information in the entry and to obtain the anti-virus state information from the entry.

22. 18
~~23.~~ (Currently amended) The computer system of claim ~~2019~~, wherein the data structure containing the anti-virus state information is an extra file fork for the file and the anti-virus process further causes the processor to store the anti-virus state information in the extra file fork and to obtain the anti-virus state information from the extra file fork.

23. 22
~~24.~~ (Currently amended) The computer system of claim ~~2423~~, wherein the anti-virus process further causes the processor to create the extra file fork to hold the anti-virus state information.

24. 18
~~25.~~ (Currently amended) The computer system of claim ~~2019~~, wherein the data structure containing the anti-virus state information is stored as a resource in a resource fork for the file and the anti-virus process further causes the processor to store the anti-virus state information in the resource fork and to obtain the anti-virus state information from the resource fork.

A1 [26. (Cancelled)]

25.
~~27.~~ (Currently amended) ~~The~~ A computer-readable medium ~~of claim 27,~~ having stored thereon a directory entry data structure for a file system comprising:

a file identifier field containing data representing a file system identifier for a file wherein the file comprises a data fork and a resource fork;

a first reserved field containing data representing an anti-virus state for the file identified by the file identifier field, the ~~first reserved field contains~~ data representing a two-byte checksum for the file and ~~data representing~~ two bytes of a three-byte length for the resource fork~~,~~; and ~~further comprising:~~

a second reserved field containing data representing a third byte for the resource fork length and data representing a three-byte length for the data fork.

[28. (Cancelled)]